IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	Pankaj MEHRA	§	Confirmation No.:	3837
Serial No.:	10/694,323	§	Group Art Unit:	2143
Filed:	10/27/2003	§	Examiner:	Mark D. Fearer
For:	Configuration Validation Checker	§	Docket No.:	200309900-1

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Date: February 19, 2008

Sir:

Appellant hereby submits this Appeal Brief in connection with the above-identified application. A Notice of Appeal was electronically filed on January 21, 2008.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is the Hewlett-Packard Development Company, L.P. (HPDC), a Texas Limited Partnership, having its principal place of business in Houston, Texas. HPDC is a wholly owned affiliate of Hewlett-Packard Company (HPC). The Assignment from the inventor to HPDC was recorded on October 27, 2003 at Reel/Frame 014644/0622.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals or interferences.

III. STATUS OF THE CLAIMS

Originally filed claims:	1-17.
Claim cancellations:	None.
Added claims:	None.
Presently pending claims:	1-17.
Presently appealed claims:	1-17.

IV. STATUS OF AMENDMENT

Appellant has not filed any amendments after the Final Office Action dated November 28, 2007.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Various embodiments of the invention are described below. The scope of disclosure is not limited by the descriptions of the embodiments that follow. Citations to the specification have been provided to demonstrate where support may be found in the specification for various parts of the invention. Additional support may be found elsewhere in the application.

Appellant's contribution is directed to a network switch 300 (Fig. 7) that is able to monitor its ports 308 and detect when a link up/down event occurs on that port 308. P. 11, ll. 4-6. An event in which a link becomes non-functional is referred to as a link "down" event. P. 10, ll. 20-21. An event in which a link is newly established is referred to as a link "up" event. P. 10, ll. 21-22. When the switch 300 detects the occurrence of a link up/down event on a port 308, the switch 300 modifies its routing behavior accordingly. P. 11, l. 4 – p. 12, l. 5.

Claim 1 is directed to a switch 300 that comprises a plurality of ports 308. Fig. 7 and p. 10, ll. 12-24. The switch 300 also comprises a plurality of link up/down detection logic units 306, where each link up/down detection logic unit 306 is associated with a port 308 and is configured to detect a change in the state of a link associated with the port 308. P. 11, ll. 4-6. The switch 300 further comprises a configuration validation checker 302 coupled to each of the link up/down detection logic units 306. Fig. 7 and p. 10, ll. 12-24. The configuration validation checker 302 causes the switch 300 to change its routing behavior with regard to a port 308 for which a link up/down detection unit 306 has detected a state change. P. 11, l. 4 – p. 12, l. 5.

Dependent claim 2 is directed to the link up/down detection logic units 306 of claim 1. Each link up/down detection logic unit 306 informs the configuration validation checker 302 when a link to an associated port 308 becomes non-functional, and the configuration validation checker 302 responds by discarding all packets. P. 11, ll. 4-10; Figure 7.

Dependent claim 3 is directed to the link up/down detection logic units 306 of claim 1, where each link up/down detection logic unit 306 informs the configuration validation checker 302 when a link to an associated port 308

becomes non-functional, and the configuration validation checker 302 responds by discarding all packets destined to that link. P. 11, ll. 4-10; Figure 7.

Dependent claim 4 is directed to the link up/down detection logic units 306 of claim 1. Each link up/down detection logic unit 306 informs the configuration validation checker 302 when a non-functional link to an associated port 308 becomes functional. P. 11, ll. 4-6; Figure 7. The configuration validation checker 302 responds by receiving an identifier value from an entity coupled to the switch 300 via the functional link and comparing the identifier value received from the entity with topology information contained in the switch 300. P. 12, ll. 6-10; Figure 7. If the identifier value matches a value in the topology information, the configuration validation checker 302 permits the switch 300 to route packets over the functional link; if the identifier value does not match a value in the topology information, the configuration validation checker 302 discards all packets targeting the functional link. P. 12, ll. 10-22; Figure 7.

Dependent claim 6 requires that if topology information contained in the switch 300 does not comport with topology information received from an external entity, the newly received topology information is prevented from being used by the switch 300. P. 12, ll. 10-22; Figure 7.

Claim 7 is directed to a switch 300 that comprises a plurality of ports 308. Fig. 7 and p. 10, ll. 12-24. The switch 300 also comprises a plurality of link up/down detection logic units 306, where each link up/down detection logic unit 306 is associated with a port 308 and is adapted to detect a change in the state of a link associated with the port 308. P. 11, ll. 4-6. The switch 300 further comprises means[1] for causing the switch 300 to change its routing behavior with

[1] 37 C.F.R. § 41.37(c)(1)(v) requires that means-plus-function claims be identified and that the "structure, material, or acts described in the specification as corresponding to each claimed function must be set forth with reference to the specification by page and line number, and to the drawing, if any, by reference characters." The means described here may refer to the configuration validation checker 302 shown in Figure 7 and described in the specification, p. 11, l. 4 – p. 12, l. 5. These means may be further described elsewhere in the specification.

regard to a port 308 for which a link up/down detection unit 306 has detected a state change. P. 11, l. 4 – p. 12, l. 5.

Dependent claim 8 is directed to the switch 300 of claim 7, but also comprises means[1] for receiving an indication from the link up/down detection logic units that a link to an associated port has become non-functional. The switch 300 further comprises means[1] for ceasing routing of all packets.

Dependent claim 9 is directed to the switch 300 of claim 7, but also comprises means[1] for receiving an indication from the link up/down detection logic units that a link to an associated port has become non-functional. The switch 300 further comprises means[1] for ceasing routing of all packets destined to that link.

Claim 10 is directed to a network that comprises a plurality of switches 100-116 (Fig. 1) coupled together and at least one end node 120-126 coupled to at least one switch. P. 3, ll. 28-31. At least one switch 300 (Fig. 7) includes a link up/down detection logic unit 306 associated with a port 308 and configured to detect a change in the state of the link. P. 11, ll. 4-6. The at least one switch 300 further includes a configuration validation checker 302 coupled to the link up/down detection logic unit 306. P. 11, l. 4 – p. 12, l. 5. The configuration validation checker 302 causes the switch 300 to change its routing behavior with regard to the port 308 if the link up/down detection unit 306 has detected a state change. P. 11, l. 4 – p. 12, l. 5.

Claim 13 is directed to a method performed by a switch 300 contained in a system 90 (Figs. 1 and 7). The method comprises the switch 300 monitoring a port 308 for a link down event or a link up event, where the link down event is indicative of a link from the switch 300 to an entity becoming non-functional and the link up event is indicative of a newly established link from the switch 300 to the entity. P. 11, ll. 4-6. The switch 300 detects a link down event associated with the switch 300 or a link up event associated with the switch 300. P. 11, ll. 4-6. The method also comprises receiving a packet into the switch 300 and the switch 300 determining if the packet is to be routed out through the port 308 associated with the detected link down event or link up event. P. 8, ll. 13-23. If

the switch determines that the packet is to be routed out through the port associated with a detected link down event, the switch discards the packet. P. 11, ll. 4-10. If the switch determines that the packet is to be routed out through the port associated with a detected link up event, the switch routes the packet through the port. P. 11, l. 21 – p. 12, l. 5.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether under 35 USC § 103(a) claims 1, 3, 7, 9-10 and 12 are obvious in view of Shabtay (U.S. Pub. No. 2004/0047336 A1) and Ball (U.S. Pub. No. 2003/0046390 A1).

Whether under 35 USC § 103(a) claims 2, 4-6, 8 and 11 are obvious in view of Shabtay, Ball and Kao (U.S. Pat. No. 7,054,951 B1).

Whether under 35 USC § 103(a) claims 13-17 are obvious in view of Sawada (U.S. Pat. No. 6,907,470 B2) and Ball.

VII. ARGUMENT

A. Summary of Ball

The relevant portion of Ball cited by the Examiner (paragraph [0020]) is directed to network segmentation. Specifically, Ball teaches that a VLAN-enabled switch segments stations connected thereto into logically defined groups. This grouping is performed on a VLAN-by-VLAN basis. Specifically, network traffic received from an end-station belonging to a particular VLAN is output only on other ports that are also associated with that VLAN. In some cases, VLANs may be defined between different domains connected by a router. In such cases, the router may pass traffic between different domains. The router also may pass traffic between VLANs in the same domain because VLANs generally do not share user information. To accomplish the foregoing, the router is configured as a member of all VLANs.

Although Ball discusses network segmentation as described above, Ball makes no mention of a switch that changes its routing behavior with regard to a port for which a link up/down detection unit has detected a state change.

The Examiner also cited paragraph [0026] of Ball. Paragraph [0026] of Ball describes the Open Shortest Path First (OSPF) network communication protocol, which is already well-known in the art. The OSPF teaches that when a router is turned on it sends “hello” (initialization) packets to all of its neighbors, receives their “hello” packets in return, and establishes routing connections by synchronizing databases with adjacent routers that agree to synchronize. At regular intervals, each router sends an update message called its "link state" describing its routing database to all the other routers, so that all routers have the same description of the topology of the local network. Each router then determines a mathematical data structure called a "shortest path tree" that describes the shortest path to each destination address and therefore indicates the closest router to send to for each communication (*i.e.*, "open shortest path first”).

B. Summary of Kao

The Examiner cited two portions of Kao. One of these portions, col. 12, ll. 27-39, describes what occurs when a query packet is received to Kao's computer system. Specifically, Kao teaches that if a query packet is received from another node, then the MAC address of the query packet is compared to the MAC address of [apparently] the node at which the query packet was received. Col. 27, ll. 27-30. If the MAC address is smaller than the node's MAC address, the query packet is forwarded to another node. Col. 27, ll. 32-35. However, if the MAC address is larger than the node's MAC address, the query packet is discarded. Col. 27, ll. 35-37. The above description applies for embodiments in which the node with the smallest MAC address sets the ring identifier for the network. Col. 27, ll. 30-32. In embodiments where the node with the largest MAC address sets the ring identifier for the network, the transitions described above are reversed. Col. 27, ll. 37-39.

The other portion of Kao cited by the Examiner, col. 13, l. 61 – col. 14, l. 5, describes the comparison of a ring identifier associated with a "topology discovery packet" matches a ring identifier associated with a ring on which a packet is received. Col. 13, ll. 60-63. Kao teaches that if no match is found, the packet is forwarded without appending any information relating to the receiving node to the topology discovery packet. Col. 13, ll. 63-66. However, if there is a match, the **address for the receiving node is appended to the topology packet**, and, optionally, the ring identifier associated with the ring on which the packet was received is appended to the topology packet as well. Col. 13, l. 67 – col. 14, l. 5.

C. Section 103 rejections in view of Shabtay and Ball

1. Combination of Shabtay and Ball fails to disclose adjustment of switch routing behavior as required by claims 1, 7 and 10

Claims 1, 7 and 10 stand rejected as allegedly obvious over Shabtay and Ball. Claim 1 is representative of this grouping of claims. The grouping should not be construed to mean the patentability of any of the claims may be determined in later actions (*e.g.*, actions before a court) based on the groupings.

Rather, the presumption of 35 USC § 282 shall apply to each of these claims individually.

Representative claim 1 requires "a configuration validation checker coupled to each of the link up/down detection logic units, said configuration validation checker causes the switch to change its routing behavior with regard to a port for which a link up/down detection unit has detected a state change." The combination of Shabtay and Ball fails to teach or suggest this limitation.

On p. 8 of the Final Office Action, the Examiner admits that Shabtay fails to teach this limitation and, as a result, the Examiner turns to Ball. The Examiner asserts that Ball teaches this limitation in paragraph [0020]. However, as demonstrated above under subsection A, Ball makes no explicit, inherent or even implicit mention of a switch that changes it routing behavior **with regard to a port for which a link up/down detection unit has detected a state change**, as required by representative claim 1. For Ball to teach this limitation, Ball would have to disclose at least a switch that has a link up/down detection unit, where the detection unit detects link-up events and link-down events. An event in which a link becomes non-functional is referred to as a link "down" event. An event in which a link is newly established is referred to as a link "up" event. Moreover, the switch would also have to change its routing behavior based on such detections. As Appellant explained above, Ball fails to teach or suggest these requirements. Shabtay fails to satisfy the deficiencies of Ball.

Based on the foregoing, Appellant respectfully submits that the rejections of the claims in this grouping be reversed, and the claims set for issue.

2. Combination of Shabtay and Ball fails to disclose the discarding of all packets destined to a link when that link becomes non-functional, as claimed in claims 3, 9 and 12

Claims 3, 9 and 12 stand rejected as allegedly obvious over Shabtay and Ball. Claim 3 is representative of this grouping of claims. The grouping should not be construed to mean the patentability of any of the claims may be determined in later actions (*e.g.*, actions before a court) based on the groupings.

Rather, the presumption of 35 USC § 282 shall apply to each of these claims individually.

Claim 3 is allowable for at least the reasons described in Section VII(B)(1) above.

Claim 3 is allowable for an additional reason. Specifically, claim 3 requires "wherein each link up/down detection logic unit informs the configuration validation checker when a link to an associated port becomes non-functional, and the configuration validation checker responds by discarding all packets destined to that link." The Office action asserts this limitation is disclosed in Shabtay, paragraph [0029]. However, this portion of Shabtay teaches that "[p]referably, the managing bridging-device is connected to the redundant link through a predetermined port" and that "...only the managing bridging-device is permitted to change the status of an operative link from active to blocked." Final Office Action, p. 9. No mention is made of "discarding all packets destined to [a] link" when that link becomes non-functional, as required by claim 3. Ball fails to satisfy the deficiencies of Shabtay.

Based on the foregoing, Appellant respectfully submits that the rejections of the claims in this grouping be reversed, and the claims set for issue.

D. Section 103 rejections in view of Shabtay, Ball and Kao

1. Combination of Shabtay, Ball and Kao fails to disclose handling of all packets in response to a link becoming non-functional as required by claims 2, 8 and 11

Claims 2, 8 and 11 stand rejected as allegedly obvious in view of Shabtay, Ball and Kao. Claim 2 is representative of this grouping of claims. The grouping should not be construed to mean the patentability of any of the claims may be determined in later actions (*e.g.*, actions before a court) based on the groupings. Rather, the presumption of 35 USC § 282 shall apply to each of these claims individually.

Claim 2 is allowable for at least the same reasons as discussed in Section VII(B)(1) above.

Further, claim 2 is allowable for an additional reason. Specifically, claim 2 requires "wherein each link up/down detection logic unit informs the configuration validation checker when a link to an associated port becomes non-functional, and the configuration validation checker responds by discarding all packets." On p. 10 of the Final Office Action, the Examiner admits that the combination of Shabtay and Ball fails to disclose such a limitation. However, the Examiner asserts that Kao, col. 12, ll. 27-39, discloses this limitation. Appellant respectfully disagrees. This portion of Kao discloses the discarding of a (presumably) single "query packet" in response to a MAC address of the query packet being greater than the MAC address of the node. In contrast, claim 2 requires that "**all** packets" (emphasis added) are discarded by the configuration validation checker in response to a link becoming "non-functional." Stated in another way, in claim 2, not only are all packets discarded (as opposed to just the query packet in Kao), but these packets are discarded in response to a link becoming non-functional (as opposed to MAC address comparison in Kao).

Based on the foregoing, Appellant respectfully submits that the rejections of the claims in this grouping be reversed, and the claims set for issue.

2. Combination of Shabtay, Ball and Kao fails to disclose routing of packets based on topology information as required by claim 4

Claim 4 stands rejected as allegedly obvious over Shabtay, Ball and Kao. Claim 4 is allowable for at least the reasons described above in Section VII(B)(1).

Claim 4 is allowable for an additional reason. Specifically, claim 4 requires "if the identifier value matches a value in the topology information, permitting the switch to route packets over the functional link" and "if the identifier value does not match a value in the topology information, discarding all packets targeting the functional link." The Examiner admits that Shabtay and Ball fail to disclose these limitations, but asserts that Kao discloses these limitations at col. 13, l. 51- col. 14, l. 5 and col. 12, ll. 27-39. Final Office Action, p. 12. The Examiner is mistaken. These portions of Kao state that if a match does arise, then information is appended to a topology packet. In contrast, claim 4 requires that if

a match arises, "permitting the switch to route packets over the functional link." Claim 4 denotes control over a switch, while Kao focuses on whether or not information is appended. Further, Kao states that if there is no match, the **packet is forwarded** without appending any information onto the topology discovery packet. In direct contrast, claim 4 requires that if there is no match, all packets targeting the functional link **are discarded**. While Kao permits the packet to be forwarded (albeit without appended information), claim 4 discards the packet. Shabtay and Ball fail to satisfy the deficiencies of Kao.

Based on the foregoing, Appellant respectfully submits that the rejections of claim 4 be reversed, and the claim set for issue.

3. Claim 5 is allowable for same reasons as discussed in Section VII(B)(1)

Claim 5 stands rejected as allegedly obvious in view of Shabtay, Ball and Kao. Claim 5 is allowable for at least the same reasons as discussed in Section VII(B)(1) above.

4. Combination of Shabtay, Ball and Kao fails to disclose preventing topology information from being used by a switch as required by claim 6

Claim 6 stands rejected as allegedly obvious in view of Shabtay, Ball and Kao. Claim 6 is allowable for at least the reasons described in Section VII(B)(1) above.

Claim 6 is allowable for an additional reason. Specifically, claim 6 requires "wherein if the topology information contained in the switch does not comport with the topology information received from the external entity, preventing the newly received topology information from being used by the switch." On p. 14 of the Final Office Action, the Examiner admits that Shabtay and Ball fail to disclose this limitation and thus turns to Kao. The Examiner asserts that Kao discloses this limitation at col. 12, ll. 27-39. Appellant respectfully disagrees. This portion of Kao discloses the discarding of a (presumably) single "query packet" in response to a MAC address of the query packet being greater than the MAC address of the node. In contrast, Appellant points out that claim 6 requires not the discarding of a packet, but "preventing the newly received topology information from being

used by the switch." In further contrast, the preventative action required by claim 6 is in response to the comparison of topology information, whereas in Kao, the discarding of the packet is in response to the comparison of MAC addresses.

Based on the foregoing, Appellant respectfully submits that the rejection of claim 6 be reversed, and the claim set for issue.

E. Section 103 rejections in view of Sawada and Ball

1. Sawada and Ball fail to disclose packet routing as claimed in claim 13

Claims 13-17 stand rejected as allegedly obvious over Sawada and Ball. Claim 13 is representative of this grouping of claims. The grouping should not be construed to mean the patentability of any of the claims may be determined in later actions (*e.g.*, actions before a court) based on the groupings. Rather, the presumption of 35 USC § 282 shall apply to each of these claims individually.

Representative claim 13 requires "if the switch determines that the packet is to be routed out through said port associated with a detected link up event, the switch routing the packet through said port." On p. 3 of the Final Office Action, the Examiner admits that Sawada fails to teach this limitation and, as a result, the Examiner turns to Ball and asserts that Ball discloses this limitation in paragraph [0026].

Appellant respectfully disagrees. Paragraph [0026] of Ball is merely a brief description of the Open Shortest Path First (OSPF) network communication protocol. As explained above, the OSPF teaches that when a router is turned on it sends "hello" (initialization) packets to all of its neighbors, receives their "hello" packets in return, and establishes routing connections by synchronizing databases with adjacent routers that agree to synchronize. At regular intervals, each router sends an update message called its "link state" describing its routing database to all the other routers, so that all routers have the same description of the topology of the local network. Each router then determines a mathematical data structure called a "shortest path tree" that describes the shortest path to each destination address and therefore indicates the closest router to send to for each communication (*i.e.*, "open shortest path first").

While paragraph [0026] of Ball does discuss OSPF, there is no mention of a switch that determines whether a packet is to be routed out through a port associated with a link-up event detected by that port and, subsequently, routes the packet through that port, as required by claim 13. Switches using OSPF update their connections using link states received from entities external to the switch. In contrast, the switch of claim 13 monitors ports for link-up and link-down events on its own and, based on this monitoring, the switch chooses how to route its packets. These techniques are entirely different from one another. Ball's technique involves passively receiving link states and updating routing tables; the technique of claim 13 involves an active monitoring for link-up and link-down events and routing packets accordingly. This difference is significant at least because the switch of claim 13 may analyze the status of its ports more quickly and because there are fewer points of failure.

Based on the foregoing, Appellant respectfully submits that the rejections of the claims in this grouping be reversed, and the claims set for issue.

F. Conclusion

For the reasons stated above, Appellant respectfully submits that the Examiner erred in rejecting all pending claims. It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's Deposit Account No. 08-2025.

Respectfully submitted,

/Nick P. Patel/

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Dept., M/S 35
P.O. Box 272400
Fort Collins, CO 80527-2400

Nick P. Patel, PTO Reg. No. 57,365
CONLEY ROSE, P.C.
(713) 238-8000 (Phone)
(713) 238-8008 (Fax)
AGENT FOR APPELLANT

VIII. CLAIMS APPENDIX

1. (Previously presented) A switch, comprising:

a plurality of ports;

a plurality of link up/down detection logic units, each link up/down detection logic unit associated with a port and configured to detect a change in the state of a link associated with the port; and

a configuration validation checker coupled to each of the link up/down detection logic units, said configuration validation checker causes the switch to change its routing behavior with regard to a port for which a link up/down detection unit has detected a state change.

2. (Original) The switch of claim 1 wherein each link up/down detection logic unit informs the configuration validation checker when a link to an associated port becomes non-functional, and the configuration validation checker responds by discarding all packets.

3. (Original) The switch of claim 1 wherein each link up/down detection logic unit informs the configuration validation checker when a link to an associated port becomes non-functional, and the configuration validation checker responds by discarding all packets destined to that link.

4. (Previously presented) The switch of claim 1 wherein each link up/down detection logic unit informs the configuration validation checker when a non-functional link to an associated port becomes functional, and the configuration validation checker responds by:

receiving an identifier value from an entity coupled to the switch via the functional link;

comparing the identifier value received from the entity with topology information contained in the switch;

if the identifier value matches a value in the topology information, permitting the switch to route packets over the functional link; and

if the identifier value does not match a value in the topology information, discarding all packets targeting the functional link.

5. (Original) The switch of claim 1 wherein said configuration validation checker receives topology information from an entity external to the switch and compares the received topology information to topology information contained in the switch.

6. (Original) The switch of claim 5 wherein if the topology information contained in the switch does not comport with the topology information received from the external entity, preventing the newly received topology information from being used by the switch.

7. (Previously presented) A switch, comprising:

a plurality of ports;

a plurality of link up/down detection logic units, each link up/down detection logic unit associated with a port and adapted to detect a change in the state of a link associated with the port; and

means for causing the switch to change its routing behavior with regard to a port for which a link up/down detection unit has detected a state change.

8. (Original) The switch of claim 7 further including a means for receiving an indication from the link up/down detection logic units that a link to an associated port has become non-functional and a means for ceasing routing of all packets.

9. (Original) The switch of claim 7 further including a means for receiving an indication from the link up/down detection logic units that a link to an associated port has become non-functional and a means for ceasing routing of all packets destined to that link.

10. (Previously presented) A network, comprising:

a plurality of switches coupled together;

at least one end node coupled to at least one switch;

wherein at least one switch includes:

a link up/down detection logic unit associated with a port and configured to detect a change in the state of the link; and

a configuration validation checker coupled to the link up/down detection logic unit, said configuration validation checker causes the switch to change its routing behavior with regard to the port if the link up/down detection unit has detected a state change.

11. (Previously presented) The network of claim 10 wherein the link up/down detection logic unit informs the configuration validation checker when the link becomes non-functional, and the configuration validation checker responds by rejecting all packets.

12. (Previously presented) The network of claim 10 further including a plurality of ports and a link up/down detection logic associated with each port, and wherein each link up/down detection logic unit informs the configuration validation checker when a link to an associated port becomes non-functional, and the configuration validation checker responds by rejecting all packets destined to that link.

13. (Previously presented) A method performed by a switch contained in a system, comprising:

the switch monitoring a port for a link down event or a link up event, said link down event indicative of a link from the switch to an entity becoming non-functional and said link up event indicative of a newly established link from the switch to said entity;

the switch detecting a link down event associated with said switch or a link up event associated with said switch;

receiving a packet into said switch;

the switch determining if said packet is to be routed out through said port associated with the detected link down event or link up event;

if the switch determines that the packet is to be routed out through said port associated with a detected link down event, the switch discarding the packet; and

if the switch determines that the packet is to be routed out through said port associated with a detected link up event, the switch routing the packet through said port.

14. (Previously presented) The method of claim 13 further including if the switch determines that the packet is to be routed out through said port associated with a detected link down event, discarding all packets received by the switch.

15. (Previously presented) The method of claim 13 further including requesting the entity to provide a unique identifier to the switch.

16. (Original) The method of clam 15 further including the switch receiving a unique identifier from the entity, comparing the unique identifier received from the entity to state information contained in the switch and, if the unique identifier from the entity does not match a value in the state information, discarding a packet destined for the entity.

17. (Original) The method of claim 16 wherein further including if the unique identifier from the entity matches a value in the state information, permitting packets destined for the entity to be routed from the switch to the entity.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.